

다음의 명령형 언어를 생각하자:

$e ::=$	n	integer
	x	variable
	$e + e$	
	$-e$	
$c ::=$	$x := e$	assignment
	$c ; c$	sequence
	repeat c until x	repetition

“**repeat** c **until** x ”는 변수 x 가 양수가 될 때 까지 c 를 반복한다.

분석의 목표는 변수가 가지는 정수가 홀수 인지 짝수인지를 분석하는 것이라고 하자.

프로그램 c 의 의미는 $(lfp F)c$ 로 정의되고

$$\begin{aligned} F &\in (Cmd \rightarrow Mem \rightarrow Mem) \rightarrow (Cmd \rightarrow Mem \rightarrow Mem) \\ Mem &= Var \xrightarrow{\text{fin}} Val \\ Val &= 2^{\mathbb{Z}} \end{aligned}$$

요약된 의미는 $(lfp \hat{F})c$ 로 정의된다

$$\begin{aligned} \hat{F} &\in (Cmd \rightarrow \hat{Mem} \rightarrow \hat{Mem}) \rightarrow (Cmd \rightarrow \hat{Mem} \rightarrow \hat{Mem}) \\ \hat{Mem} &= Var \xrightarrow{\text{fin}} \hat{Val} \\ \hat{Val} &= \{\perp, \top, \mathbf{e}, \mathbf{o}\} \\ \hat{m}_1 \sqsubseteq \hat{m}_2 &\stackrel{\text{def}}{=} \forall x \in \text{dom}(\hat{m}_1) \cup \text{dom}(\hat{m}_2) : \hat{m}_1 x \sqsubseteq \hat{m}_2 x \\ \forall x \notin \text{dom}(\hat{m}) : \hat{m} x &\stackrel{\text{def}}{=} \perp_{\hat{Z}} \end{aligned}$$

1. 갈로아 연결

$$Val \xrightleftharpoons[\alpha_V]{\gamma_V} \hat{Val}$$

은

$$\alpha_V(X) = \begin{cases} \perp & \text{if } X = \emptyset \\ \mathbf{e} & \text{if } \forall x \in X : x \text{ is even.} \\ \mathbf{o} & \text{if } \forall x \in X : x \text{ is odd.} \\ \top & \text{otherwise} \end{cases}$$

2. 갈로아 연결

$$(Cmd \rightarrow Mem \rightarrow Mem) \xrightleftharpoons[\alpha]{\gamma} (Cmd \rightarrow \hat{Mem} \rightarrow \hat{Mem})$$

은 부품 공간들 사이의 갈로아 연결

$$Cmd \xrightleftharpoons[id]{id} Cmd \quad Var \xrightleftharpoons[id]{id} Var \quad Val \xrightleftharpoons[\alpha_V]{\gamma_V} \hat{Val}$$

을 가지고 다음과 같이 정의한다:

$$Mem = Var \xrightarrow{\text{fin}} Val \xrightleftharpoons[\alpha_M]{\gamma_M} Var \xrightarrow{\text{fin}} \hat{Val} = \hat{Mem}$$

인 α_M 는

$$\alpha_M(m) = \alpha_V \circ m \circ \gamma_{Var} = \alpha_V \circ m$$

이고

$$Mem \rightarrow Mem \xleftarrow[\alpha_C]{\gamma_C} \hat{M}em \rightarrow \hat{M}em$$

인 α_C 는

$$\alpha_C(x) = \alpha_M \circ x \circ \gamma_M$$

이며, α_M, α_C 를 가지고 위의 α 는

$$\alpha(\mathcal{C}) = \alpha_C \circ \mathcal{C} \circ \gamma_{Cmd} = \alpha_C \circ \mathcal{C}.$$

로 정의하면 갈로아 연결이 된다.

3. F 와 \hat{F} 를 정의하자.

$$\begin{aligned} F\mathcal{C}(\text{repeat } c \text{ until } x)m &= ((\mathcal{C}cm)(x) \ni x \leq 0 ? \mathcal{C}(\text{repeat } c \text{ until } x)(\mathcal{C}cm) : \emptyset) \\ &\quad \cup ((\mathcal{C}cm)(x) \ni x > 0 ? \mathcal{C}cm : \emptyset) \\ \hat{F}\hat{\mathcal{C}}(\text{repeat } c \text{ until } x)\hat{m} &= (\hat{\mathcal{C}}(\text{repeat } c \text{ until } x)(\hat{\mathcal{C}}c\hat{m})) \sqcup (\hat{\mathcal{C}}c\hat{m}) \end{aligned}$$

4. $lfp\hat{F}$ 가 $lfpF$ 의 안전한 요약임을 보이려면

$$\alpha(lfpF) \sqsubseteq lfp\hat{F}$$

임을 고정점 귀납법(*fixpoint induction*)으로 직접 증명하던가, Fixpoint Transfer 정리를 이용할 수 있으므로 다음을 증명하기만 하면 된다:

$$\alpha \circ F \sqsubseteq \hat{F} \circ \alpha.$$

즉,

$$\alpha(F\mathcal{C}) \sqsubseteq \hat{F}(\alpha\mathcal{C}).$$

모든 명령문에 대해서 위의 사실을 증명하면 되는데, 여기서는 “repeat c until x ”에 대해서만 증명해 보자. $r \stackrel{\text{let}}{=} \text{“repeat } c \text{ until } x\text{”}$ 로 하고 다시 쓰면, 증명할 것은, 임의의 \hat{m} 에 대해서

$$\alpha(F\mathcal{C})r\hat{m} \sqsubseteq \hat{F}(\alpha\mathcal{C})r\hat{m}.$$

이제 좌변을 α 의 성질을 이용해서 전개해 보면 우변보다 작거나 같게 된다:

$$\begin{aligned} \alpha(F\mathcal{C})r\hat{m} &= (\alpha_C \circ (F\mathcal{C}))r\hat{m} && \text{(by def. of } \alpha) \\ &= (\alpha_C(F\mathcal{C}r))\hat{m} \\ &= (\alpha_M \circ (F\mathcal{C}r) \circ \gamma_M)\hat{m} && \text{(by def. of } \alpha_C) \\ &= \alpha_M(F\mathcal{C}r(\gamma_M\hat{m})) \\ &\sqsubseteq \alpha_M(\mathcal{C}r(\mathcal{C}c(\gamma_M\hat{m})) \cup \mathcal{C}c(\gamma_M\hat{m})) && \text{by def. of } F \\ &= \alpha_M(\mathcal{C}r(\mathcal{C}c(\gamma_M\hat{m}))) \sqcup \alpha_M(\mathcal{C}c(\gamma_M\hat{m})) && \text{by Galois conn.} \\ &\sqsubseteq (\alpha\mathcal{C})r(\alpha_M(\mathcal{C}c(\gamma_M\hat{m}))) \sqcup (\alpha\mathcal{C})c(\alpha_M(\gamma_M\hat{m})) && \text{by Prop.1 twice} \\ &\sqsubseteq (\alpha\mathcal{C})r((\alpha\mathcal{C})c(\alpha_M(\gamma_M\hat{m}))) \sqcup (\alpha\mathcal{C})c(\alpha_M(\gamma_M\hat{m})) && \text{by Prop.1 twice} \\ &\sqsubseteq (\alpha\mathcal{C})r((\alpha\mathcal{C})c\hat{m}) \sqcup (\alpha\mathcal{C})c\hat{m} && \text{by Galois conn.} \\ &= \hat{F}(\alpha\mathcal{C})r\hat{m}. \end{aligned}$$

Proposition 1 $f \in A \rightarrow B$ 는 단조함수이고 $A \xrightleftharpoons[\alpha_A]{\gamma_A} \hat{A}$ 이고 $B \xrightleftharpoons[\alpha_B]{\gamma_B} \hat{B}$ 일 때,

$$\alpha_B(f a) \sqsubseteq (\alpha_{A \rightarrow B} f)(\alpha_A a)$$

이다. 왜냐하면,

$$\begin{aligned} \alpha_B(f a) &\sqsubseteq \alpha_B(f(\gamma_A(\alpha_A a))) \\ &= (\alpha_B \circ f \circ \gamma_A)(\alpha_A a) \\ &\sqsubseteq (\alpha_{A \rightarrow B} f)(\alpha_A a). \end{aligned}$$